UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/734,083	12/11/2003	Richard Lippmann	MIS-00301	7971

7590 01/06/2006

Muirhead and Saturnelli, LLC
200 Friberg Parkway
Suite 1001
Westborough, MA 01581

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 01/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/734,083	LIPPMANN ET AL.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 June 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31 and 59-89* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31 and 59-89* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20051202*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-31 and 59-89 are pending.

2. Amendment filed 12/02/2005 has been received and considered.

Claim Rejections - 35 USC § 101

3. The rejections made under 35 U.S.C. 101 have been withdrawn based on the filed amendment.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-10, 16-24, 25-31, 59-64, 65-68, 74-89 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier (US 5850516) in view of Steffan et al ("Collaborative Attack Modeling").

As per claims 1 and 59, Schneier discloses generating an attack tree by receiving a starting point of a computer attack

with respect to said network (see column 5 lines 9-15 and column 6 lines 25-47); inserting a root node into said attack tree for said starting point and determining whether, for a current node included in said attack tree to add to said attack tree a resulting node and an edge connecting said current node to said resulting node if said edge and said resulting node are not already included in said augmented attack tree with said edge connecting an ancestor of the current node to an instance of the resulting node; and inserting nodes and edges into said attack tree in accordance with said determining, said determining being repeatedly performed for nodes inserted into said attack tree, said inserting being repeatedly performed in accordance with said determining (see column 11 lines 10-46).

Schneier fails to disclose the pruned augmented attack tree is a pruned version of the full attack tree.

However, Steffan et al teaches pruning an attack tree (see section 3.1 and section 5).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to prune Schneier's attack tree.

Motivation to do so would have been that it is advantageous to prune non-relevant sub-graphs when a condition is not fulfilled (see section 5).

As per claims 2 and 60, the modified Schneier and Steffan et al system discloses the pruned augmented attack tree is a tree including n levels, said starting point being a root of said tree at level 0, n being at least 0 (see Schneier column 6 lines 25-47 and figures 3-4).

As per claims 3 and 61, the modified Schneier and Steffan et al system discloses said pruned augmented attack tree represents information about at least one of: an attacker state including a host and an attacker access level on said host, and a network state (see Schneier column 6 lines 25-47 and figures 3-4).

As per claims 4 and 62, the modified Schneier and Steffan et al system discloses an edge from a first node at level x to a second node at level x+1 represents an action while in a first state including a first attacker state corresponding to said first node resulting in a second state including a second attacker state (see column 6 lines 25-47).

As per claims 5-6 and 63-64, he modified Schneier and Steffan et al system discloses said action exploits a vulnerability on a host in said network wherein said first attacker state represents a first host and a first attacker access level on said first host, and said second attacker state represents at least one of: a second host and a second attacker

access level on said second host, and said first host and a second attacker access level on said first host wherein said second attacker access level represents at least one of: an increase in attacker privilege, an increase in attacker access, and an increase in attacker knowledge (see Schneier column 6 lines 25-47).

As per claims 7-8 and 65-66, the modified Schneier and Steffan et al system discloses said current node is at a level n, and said ancestors of said current node are located at levels in said pruned augmented attack tree at a level less than n and said pruned augmented attack tree is generated using a breadth first search technique in which nodes are added to said pruned augmented attack tree at an nth level prior to adding any node from level n+1 to said pruned augmented attack tree (see Schneier column 6 lines 25-47 and figures 3-4).

As per claims 9 and 67, the modified Schneier and Steffan et al system discloses a plurality of computer attack paths for said network are represented using a plurality of pruned augmented attack trees, each of said pruned augmented attack trees representing computer attack paths originating from a unique starting point (see Schneier column 6 lines 25-47 and figures 3-4).

As per claims 10 and 68, the modified Schneier and Steffan et al system discloses said starting point is one of: from within said network and external to said network (see Schneier column 6 lines 25-47 and figures 3-4).

As per claims 16 and 74, the modified Schneier and Steffan et al system discloses said generating uses connectivity information, said connectivity information including a connection between two endpoints representing elements of a configuration of said network (see Schneier column 6 lines 25-47 and figures 3-4 and Steffan section 3.1).

As per claims 17 and 75, the modified Schneier and Steffan et al system discloses said connectivity information includes physical connectivity between network interfaces and logical connectivity through network communications protocols (see Schneier column 6 lines 25-47 and figures 3-4 and Steffan section 3.1).

As per claims 18-19 and 76-77, the modified Schneier and Steffan et al system discloses said connection is associated with a path including one or more hops wherein each of said one or more hops is associated with at least one of: a filtering rule, a translation rule, and an interface of a host in said network (see Schneier column 6 lines 25-47 and figures 3-4 and Steffan section 3.1).

As per claims 20-22 and 78-80, he modified Schneier and Steffan et al system discloses at least one of said endpoints is associated with a vulnerability on said at least one endpoint wherein said vulnerability has an associated action resulting in exploitation of said vulnerability wherein said associated action is related to an entity representing at least one of: an attacker access level, attacker knowledge level, a change to a network state (see Schneier column 6 lines 25-47).

As per claims 23-24 and 81-82, he modified Schneier and Steffan et al system discloses said pruned augmented attack tree is used to determine an effect of preventing at least one action (see Schneier column 17 line 61 through column 18 line 3) and modifying said pruned augmented attack tree in accordance with eliminating at least one action in connection with a vulnerability associated with said host producing a modified augmented attack tree; and evaluating said modified augmented attack tree (see Schneier column 7 lines 39-52).

As per claims 25 and 83, the modified Schneier and Steffan et al system discloses connectivity data representing connectivity between pairs of endpoints in said network is used by said generating, and the method further comprising: automatically generating said connectivity data in accordance with at least one translation rule, at least one filtering rule,

and network configuration information (see Schneier column 6 lines 25-47 and figures 3-4 and Steffan section 3.1).

As per claims 26 and 84, the modified Schneier and Steffan et al system discloses said at least one translation rule includes at least one of: an address translation rule and a port translation rule (see Schneier column 6 lines 25-47 and figures 3-4 and Steffan section 3.1).

As per claims 27 and 85, the modified Schneier and Steffan et al system discloses selecting at least one address of a starting point of a computer attack using at least one rule; and determining a portion of said connectivity data using said at least one address (see Schneier column 6 lines 25-47 and figures 3-4 and Steffan section 3.1).

As per claims 28-30 and 86-88, the modified Schneier and Steffan et al system discloses said at least one rule includes at least one of a filtering rule and a translation rule and said at least one address is used in said generating to represent an alternate connectivity of a host said address is one of an address in accordance with a communications protocol and an address associated with said network (see Schneier column 6 lines 25-47 and figures 3-4 and Steffan section 3.1).

As per claims 31 and 89, he modified Schneier and Steffan et al system discloses using vulnerability data to determine at

least one of: requirements for an action, an attacker state resulting from an action, and a network state resulting from an action, where said requirements include a locality describing whether a vulnerability can be exploited remotely over a network or locally on a host, said resulting attacker state includes an effect describing an access level or privilege or knowledge after an exploit of a vulnerability, and said resulting network state includes a denial of service describing a loss of service on a host after an exploit of a vulnerability (see Schneier column 6 lines 25-47).

6. Claims 13 and 71 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier and Steffan et al system as applied to claims 1 and 59 above, and further in view of Swiler et al (Computer-Attack Graph Generation Tool).

As per claims 13 and 71, the modified Schneier and Steffan et al system fails to disclose said pruned augmented attack tree has a property that a resulting node at a level "n+1" and an edge connecting a current node at level "n" to said resulting node are included in said pruned augmented attack tree if said edge and said resulting node are not already included in said pruned augmented attack 5 tree with said edge connecting an ancestor of the current node to an instance of the resulting

node, said ancestor being a node at a level "x" < "n" and said instance of the resulting node being at level "x+1".

However, Swiler teaches such a property (see section 3.3).

At the time of the invention it would have been obvious to a person of ordinary skill in the art for the modified Schneier and Steffan et al systems graphs to have the property of Swiler's graphs.

Motivation to do so would have been to ensure that large graphs could be analyzed (see section 3.3).

7. Claims 14 and 72 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier and Steffan et al system as applied to claims 1 and 59 above, and further in view of Ammann et al (Scalable, Graph-Based Network Vulnerability Analysis).

As per claims 14 and 72, the modified Schneier and Steffan et al system fails to disclose determining which hosts in said network are equivalent forming a group; and representing said group with a single host.

However, Ammann teaches such grouping (see page 223 right column).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to group similar hosts in the modified system of Schneier and Steffan et al.

Motivation to do so would have been to simplify the attack graph (see Ammann page 223 right column).

8. Claims 11-12 and 69-70 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier and Steffan et al system as applied to claims 6 and 64 above, and further in view of Swiler et al.

As per claims 11-12 and 69-70, the modified Schneier and Steffan et al system fails to disclose evaluating each action that exploits a vulnerability of a host in accordance with connectivity data wherein said connectivity data, said each action, and said vulnerability are stored in a database and determined prior to performing said generating.

However, Swiler teaches evaluating each action that exploits a vulnerability of a host in accordance with connectivity data (see section 2.2) wherein said connectivity data, said each action, and said vulnerability are stored in a database and determined prior to performing said generating (see sections 3.1 and 3.2.1).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Swiler's data collection and storing method in the modified system of Schneier and Steffan et al.

Motivation to do so would have been that commercial tools primarily use databases to store results (see section 3.2.1).

Response to Arguments

9. Applicant's arguments with respect to claims 1-31 and 59-89 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137